COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

WENDY L. WATANABE
AUDITOR-CONTROLLER

May 22, 2013

TO: Marvin J. Southard, D.S.W., Director
Department of Mental Health

FROM: Wendy L. Watanabe
Auditor-Controller

SUBJECT: **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT COMPLIANCE REVIEW – EDELMAN'S CHILDREN'S MENTAL HEALTH PROGRAM**

We have completed a Health Insurance Portability and Accountability Act (HIPAA) compliance review of the Department of Mental Health (DMH) Edelman's Children's Mental Health Program (ECMHP or Program), a HIPAA covered program. Our review was prompted by prior findings of non-compliance during an unannounced site visit to ECMHP. This report details our findings.

We reviewed our report with DMH management, who agreed with our findings and declined a formal exit conference.

Background

On July 26, 2012, we conducted an unannounced site visit to ECMHP as part of our effort to ensure that the County's HIPAA covered programs and clinics are posting their Notice of Privacy Practices (NPP) in prominent patient locations, as required. We noted that ECMHP did not post the NPP as required. However, hard copies of the NPP were available upon request from the receptionist. At the time of the unannounced visit, the Program Head was not available to discuss the deficiency. We subsequently informed the DMH Privacy Officer of the compliance issue, and initiated a full HIPAA compliance review of ECMHP.

On April 18, 2013, we conducted a comprehensive review to evaluate ECMHP's compliance with the HIPAA Privacy Rule, and DMH's HIPAA policies and procedures. We also used the *HIPAA Privacy Rule and Health Information Technology for Economic Clinical Health (HITECH) Act Audit Tool* in evaluating the facility's compliance. DMH

management is responsible for establishing and maintaining internal compliance with the HIPAA regulations, and has oversight of their HIPAA compliance throughout DMH facilities. We considered DMH's internal controls over their compliance program, and the HIPAA Privacy Rule requirements that could have a direct and material effect on ECMHP.

Summary of Findings

Notice of Privacy Practices

The HIPAA Privacy Rule requires a covered entity, such as the County, with direct treatment relationships with patients to give the NPP to every patient no later than the date of first service delivery, and to make a good faith effort to obtain written acknowledgment of receipt of the notice. If the provider maintains an office or other physical site where health care is provided directly to patients, the provider must also post the notice in the facility in a clear and prominent location where patients are likely to see it, as well as make the notice available to those who ask for a copy.

Our follow-up review found that ECMHP posted the NPP in the patient waiting area where patients and visitors are likely to see it. ECMHP management verified that all patients are provided with the NPP on their first service delivery date. We reviewed six randomly selected patient charts, and noted they all included the required acknowledgement of receipt.

While ECMHP was not in compliance with NPP standards at the time of our unannounced site visit, the Program Head and DMH's Privacy Officer addressed the deficiency, and was fully compliant at the time of this review.

Safeguards for Protected Health Information

A covered entity must have in place appropriate administrative, physical, and technical safeguards to protect the privacy of protected health information (PHI). A covered entity must make reasonable efforts to safeguard PHI, electronic PHI, and prevent any intentional or unintentional use or disclosure that violates the Privacy Rule.

We reviewed the following DMH policies and procedures:

- DMH Policy 500.21, *Safeguards for Protected Health Information*, which establishes administrative, physical, and technical safeguards to protect the confidentiality of PHI.

- DMH Policy 302.14, *Networked Information Systems Usage*, which governs the use of DMH information technology resources and communicates to DMH

workforce members their responsibility for acceptable use of DMH information technology resources.

ECMHP management reported that their computers are protected by endpoint protection software, which blocks downloading of PHI to portable storage devices. In addition, ECMHP's computers are configured to prevent workforce members from saving PHI onto their hard drives.

During our review, we noted that the computer monitor located at the front office and used by the receptionist is turned away from visitors and/or patients. Medical records are stored in a closet, which is locked when the custodian of records is away from the area, and access is appropriately restricted to authorized Program staff. Medical charts are tracked manually by the custodian of records. To ensure that all files are accounted for, the custodian of records will remind staff that they must return the charts by the end of the business day. Medical records are not permitted to be removed from the premises.

Confidential communications with patients and their representatives are conducted in privacy rooms, and voices are kept low in order to prevent incidental disclosures of PHI. Fax machines are located away from patients and visitors. Employees also follow the applicable policy when faxing confidential information, and verify that the intended recipient is in receipt of the fax, and promptly retrieved it from the fax location.

To the extent that we were able to review ECMHP's administrative and technical controls over PHI, the Program appears to be in compliance.

Training

The Program, as covered by HIPAA, must train its entire workforce on policies and procedures related to PHI that are required by the HIPAA Privacy and Security Rules, and to the extent necessary and appropriate for the members of its workforce to carry out their functions. Workforce members include employees, volunteers, and trainees.

The DMH Human Resources Division is responsible for ensuring its workforce members are trained on HIPAA compliance, and DMH policies and procedures via the Learning Net. Program management is responsible for providing additional role-based training for their workforce members.

Our review of ECMHP's HIPAA training records noted that Program is in compliance with the training standards. At the time of the review, all workforce members (15 employees) met the HIPAA training requirements.

Complaint Process

A covered entity must provide a process for patients to make complaints concerning the covered entity's policies and procedures. A covered entity must document all complaints received and their disposition, if any.

ECMHP management informed us that they currently follow DMH Policy 500.11, *HIPAA Privacy Complaints*, in handling patient complaints. Patients are directed to contact the Program Head or the Patients' Rights Office to file a complaint.

The ECMHP complaint process complies with HIPAA standards. We observed that the Program Head's name and contact information are posted on the registration window in the patient waiting area, to allow patients to voice their concerns regarding treatment or privacy issues. In addition, the DMH NPP posted in the waiting area informs patients that they may file a complaint with the U.S. Department of Health and Human Services (HHS), the County's Chief HIPAA Privacy Officer, or the DMH Patients' Rights Office. HIPAA complaint forms were available in the brochure racks at the patient waiting area.

Refraining from Intimidating or Retaliatory Acts

It appears that ECMHP is in compliance with the non-retaliation standards. Our discussions with ECMHP management confirmed they are aware of and understanding the importance of complying with DMH Policy 500.18, *Refraining from Retaliatory or Intimidating Acts Against Individuals That Assert Rights Under HIPAA*. Further, they understand that the Office for Civil Rights (OCR) will investigate any complaint against a covered entity that asserts retaliatory actions. No complaints related to retaliatory or intimidating acts were filed with the County's Chief HIPAA Privacy Officer by ECMHP patients.

Uses and Disclosures Requiring an Authorization

The OCR defines an authorization as a detailed document that gives covered entities permission to use PHI for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose PHI to a third party specified by the patient. An authorization must specify a number of elements, including a description of the PHI to be used and disclosed, the person authorized to make the use or disclosure, the person to whom the covered entity may make the disclosure, an expiration date, and, in some cases, the purpose for which the information may be used or disclosed.

ECMHP management indicated that workforce members understand DMH Policy 500.1, *Use and Disclosure of Protected Health Information Requiring Authorization*, and are following the policy. The purpose of our review was to ensure that ECMHP is able to refer to its Department's policy regarding uses and disclosures of PHI.

We examined the *Authorization for Request or Use/Disclosure of Protected Health Information (PHI)* form as part of this review, and determined that it meets HIPAA requirements. It appears that ECMHP is in compliance with the Uses and Disclosures Requiring Authorization standards.

Accounting for Disclosures of Protected Health Information

A patient has a right to receive an accounting of PHI disclosures made by a covered entity, and covered entities must account for certain non-routine disclosures of PHI. The Privacy Rule gives patients the right to request and receive an accounting of all disclosures of their PHI made by the covered entity, with certain exceptions, up to six years after the disclosure. In addition, an accounting of disclosures log must be maintained in each patient's medical chart.

ECMHP management reported that workforce members follow DMH Policy 500.06, *Accounting of Disclosures of Protected Health Information,* account for all disclosures of PHI, including those with authorizations, and maintain logs in patients' medical charts.

Our review of six patient accounting tracking sheets, provided by the facility, noted that the documentation meets the HIPAA requirements. It appears that ECMHP is in compliance with the Accounting for Disclosures of PHI standards.

Minimum Necessary Rule

When using, disclosing, or requesting PHI from another covered entity, a covered entity must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The Privacy Rule requires covered entities to make reasonable efforts to limit use, disclosure of, and any requests for PHI to the minimum necessary to accomplish the intended purpose for disclosure. OCR provides covered entities with flexibility to address their unique circumstances, and make their own assessment of what PHI is reasonably necessary for a particular purpose.

Discussions with ECMHP management indicate that workforce members are aware of the minimum necessary standards. It appears that ECMHP is in compliance with the minimum necessary standards.

HITECH Act Breach Notification

HHS issued regulations requiring health care providers, health plans, and other HIPAA covered entities to notify patients when their health information is breached. These "breach notification" regulations implement provisions of the HITECH Act, passed as part of the American Recovery and Reinvestment Act of 2009. The regulations developed by HHS require health care providers and other HIPAA covered entities to

promptly notify affected patients of a breach, as well as the HHS Secretary and the media in cases where a breach affects more than 500 patients. Breaches affecting fewer than 500 patients will be reported to the HHS Secretary on an annual basis. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate.

ECMHP management informed us that they trained workforce members on DMH Policy 500.28, *Responding to Breach of Protected Health Information*, which provides clear guidelines and procedures to workforce members in the event a breach or suspected breach of PHI is discovered. We reviewed the policy and established that it provides appropriate guidance to workforce members. In addition, no breaches were reported from ECMHP to the County's Chief HIPAA Privacy Officer or OCR in the past year. It appears that ECMHP is in compliance with the HITECH Act Breach Notification standards.

Conclusion

Overall, our review indicates that ECMHP management is complying with HIPAA and HITECH Act requirements to protect patient confidentiality and safeguard PHI.

We thank DMH's Audit and Compliance Division and ECMHP staff for their cooperation and assistance during this review.

Please call me or your staff may contact Linda McBride, Chief HIPAA Privacy Officer, at (213) 974-2166 if you have any questions.

WLW:RGC:GZ:LTM

c: William T Fujioka, Chief Executive Officer
John F. Krattli, County Counsel
Richard Sanchez, Chief Information Officer
Robert Pittman, Chief Information Security Officer, Chief Information Office
Judith L. Weigand, Compliance Officer, Department of Mental Health
Veronica Jones, Privacy Officer, Department of Mental Health
Ginger Fong, Privacy Officer, Department of Mental Health
Audit Committee
Health Deputies